

## REMARKS

Applicant has carefully considered the Office Action of June 22, 2004. The present response is intended to fully address all points of objection raised by the Examiner, and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application are respectfully requested.

The text has been amended at page 5 to indicate the more general description "character string", which is intended to convey a more precise definition alongside the term "word".

The claims have been amended to further clarify the inventive features which provide patentable subject matter. All of the claim amendments are fairly supported by the original text, and it is believed that no new matter has been added.

Claims 1-9, 15-16 and 18-22 inclusive have been amended. No claims have been deleted. Therefore, all of the claims 1-22 remain in the case.

The Abstract has been amended to meet formal requirements.

The principal objects of the Applicant's invention are to achieve, in an online authentication procedure:

- prevention of theft of passwords and other sensitive information whether by an online intruder, by hacking or by means of a Trojan or other "spyware" or by other online means or by an unauthorized person who may gain physical access to the user's computer
- complete portability of the method so that it is not restricted to a specific programmed computer, but rather, so that it can be used on any computer equipped with a compatible operating system.
- a means for conversion of encrypted messages to audio tones

- a means for enabling encrypted communication using keys stored on an external medium completely isolated from the user's computer.

The above objects are achieved by the present invention by provision of a self-contained program on a card in the form of CD or similar device which generates an encrypted message or Cybercoupon while the user's computer is offline without storing any passwords, or other components of the method on the user's computer and without communicating the password or other sensitive information online in order to gain access to a remote computer. Further protection is provided by disconnecting the card from the computer, while the computer is connected online.

The Examiner has rejected the Applicant's claims alternatively under Sec. 102(a) as being anticipated by Flitcroft et al, or under Sec. 103(a) as being unpatentable over Flitcroft in view of Franklin.

Neither Franklin's nor Flitcroft's methods are designed to achieve the Applicant's abovementioned objectives. In the prior art documents cited above, some elements are stored on the user's computer and are therefore subject to hacking and preclude portability. The methods can be used only in conjunction with a designated programmed computer. For example in Franklin's patent, the certificate store 50 or private key store is located on the customer computer 28. Under the heading "general operation" Franklin's patent states "The customer account number and customer-related secret are also stored at the customer computer in a password-secured storage location." It also states "The operating system 48 includes a private key store 50."

Flitcroft et al, in para. 148 refers to encrypted credit card numbers that are stored on a computer's hard disk and para. 154 states "The installation process will allow the

program to be installed a restricted number of times after which critical data is overwritten". The fact that the data can be overwritten in itself poses a security risk.

Franklin's patent 6,000,832 consciously excludes a physical card. The abstract states specifically "The "card" does not exist in physical form, but instead exists in digital form". By contrast, the Applicant's invention is specific in defining a physical credit card. The patent also requires installation of a software program on the user's computer together with a private key (parag 15 to 35). The customer computer 28 and bank computing center 32 both store the customer's private key and any additional customer-related secrets, thereby establishing secrets that are known to both the customer and issuing bank. This aspect also restricts portability as the system can be used only on the computer on which the program is stored.

Flitcroft's application 2003/00282481 of Feb. 6, 2003 is based on the use of almost identical proxy numbers as in Franklin's patent and Flitcroft's electronic embodiment poses similar security risks in the installation of software on the user's computer and the use of passwords to gain access to the software (para. 0154) on the computer. Examination of the text indicates a great similarity to Franklin.

Flitcroft's para. 0151 unambiguously provides that the numbers can only be accessed on the machine on which the software was first installed, thus preventing the unique portability which is one of the important objects of the Applicant's patent.

Flitcroft's use of a swipe card does not isolate sensitive data on the user's computer from online intrusion. Use of a swipe card is incidental as described in his paragraph 069 which merely shows how credit card transactions can originate from a merchant in the conventional manner, i.e. to communicate a credit card number online to a merchant or to a POS station.

In view of the significant differences between the Applicant's invention as detailed below, and the prior art cited by the Examiner, it could not have been obvious to a person having ordinary skill in the art to arrive at the method of the present invention. Had the novel features which are enumerated herein been obvious, one would expect that there would have been at least some hint or passing reference in one of the cited documents to their advantages.

A careful reading of Flitcroft's application shows that it deals principally with credit card numbers not cards. It is also limited to credit card applications, not general access cards as in the Applicant's invention which is designed as a general means for authentication in establishing online communication and in which credit cards comprise only a subset of the applications. Flitcroft's claims 1 to 10 inclusive refer to credit card numbers, not credit cards. Only the last claim, i.e. claim 11 refers to an actual physical card. This claim reads: "The method of claim 10, wherein said limited use credit card number is placed on a non-embossed card." Flitcroft does not even indirectly suggest a card that contains any computing circuitry. The text states explicitly that the method stores numbers, which have been received already encrypted by the issuer as confirmed in para. 072 which states that these limited use numbers can be electronically downloaded to a user's personal computer 104, where they are stored in local memory 142 of the personal computer 104 for subsequent use, constituting a risk that is avoided by the Applicant.

It would therefore not be at all obvious to combine Flitcroft system with Franklin's so that the encrypted Cybercoupons or surrogate numbers can be generated in the cards themselves. There is nothing in the text to even hint at or suggest this possibility or even a realization that it would be desirable. Had it been obvious, no doubt Flitcroft would have

made reference to this possibility as was done in respect of other possibilities such as MOTO etc.

In view of the foregoing considerations, the Applicant's invention is far from an obvious combination of Flitcroft and Franklin. The Applicant's entire invention is based on unique features, which are not hinted at in any of the cited patents. By its provision for storing the number generating program on a portable device such as a CD, and avoiding the need to store critical data or programs on the user's computer it eliminates the possibility of intrusion and enables complete portability. Another novel feature is the provision of a means for advertising, which differs significantly from the manner in which advertising is mentioned by Flitcroft et al and Franklin as detailed below under the heading Re: claims 2 and 3.

#### Detailed response

In order to respond in sequence to the Examiner's objections and to further clarify the novelty and non-obviousness of the Applicant's invention over the prior art, the following points are reiterated in more detail:

#### **1) Sec. 102(a)**

**Re: claims 1, 7-8, and 10-22, rejected under 35 U.S.C. 102(a) as being anticipated by Flitcroft et al, US Patent Application Publication No. US 2003/0028481 A1.**

Flitcroft's paras. 72 and 327 do not relate to essential features of the Applicant's invention such as operation by means of a program stored on a user's physical card while completely avoiding the storage of any component of said user program on a computer. The cited paragraphs merely refer to a means for storing numbers (not an executable program) which have been generated by the issuer, in plain language, or encrypted, and communicated to the user for storage by the

user on a PC or on a smartcard. Contrary to the above mentioned essential requirement of the Applicant's invention that no component of the program be stored on the user's computer, Flitcroft specifically does require that a program or program segments be installed on the user's computer. See also Flitcroft 68, 116 and 118.

Furthermore, Flitcroft 123 and 125 refer to the issuer communicating available numbers to the user, whereas, for security reasons, the Applicant's invention is designed specifically to avoid the communication of such numbers electronically between the issuer and the user. The Applicant specifically avoids all communication between the user and card issuer while generating the encrypted message or Cybercoupon.

**Re: Claim 20** Non-digital version, please see claims 20 and 7, below.

**Re: Flitcroft para. 72:**

In Flitcroft's electronic embodiment the numbers are electronically downloaded to a user's personal computer 104. This is clearly dissimilar to the Applicant's invention. Flitcroft paras. 0024 and 0072 require the generation of limited use credit card numbers by the issuer, not the user. The numbers must therefore be conveyed to the user by some communication means. All the above electronic methods expose the information to hacking. The Applicant avoids this danger as the Cybercoupon is generated by the user by means of a program installed on the card itself while disconnected from the internet.

**Re: Flitcroft para. 74:**

This portion describes a method for allocating proxy numbers by the issuer. It does not resemble the generation of

proxy numbers by the user as described by the Applicant. Flitcroft para. 119 describes password-controlled access to software on the user's computer, which constitutes a security risk that is deliberately overcome in the Applicant's method in which password access to the user's computer or to the issuer is avoided. In the Applicant's invention, a password is used to gain access only to the removable card, (not to the computer) in order to generate a proxy number while offline, completely isolated from online intrusion. No passwords or password recognition modules are stored on the computer and the password is not transmitted online.

**Re: Flitcroft para. 70:**

The CPU and database described in Flitcroft para. 70 differ materially from the provisions of the Applicant's invention in which the database serves a significantly different purpose from that in Flitcroft et al.

**Re: Flitcroft para. 283-302. 117-130 and para. 56-57:**

It is unclear how Flitcroft paras. 283 to 302, which contain a general description of known means of conducting purchases by Mail Order or Telephone Orders, relate to the Applicant's claim 1. These paragraphs do not disclose any features, which anticipate the Applicant's invention. Flitcroft paras. 117 to 130 dealing with electronic use of credit card numbers describe a computer-like device with password control for access to the software and initiating automated request from software to card issuing organization [125] and secure communication between software package and card issuing organization all of which constitute security risks that are deliberately circumvented in the Applicant's invention. None of these cited paragraphs anticipate the Applicant's invention.

Flitcroft's method clearly does not provide for, nor envisage installing a number generating and encryption program on an external device, completely isolated from the internet or other online connection. Contrary to an essential feature of the Applicant's design, Flitcroft requires software installed on a user's computer. Para. 0154 states "The installation process will allow the program to be installed a restricted number of times after which critical data is overwritten". The fact that the data can be overwritten in itself poses a security risk. It continues, "The precise number of allowable installations will be easily alterable within the software design. Once installed on the host computer, the program encrypts internal information regarding the machine's configuration, (note it does not encrypt the proxy numbers)". .. (Step 622). This is required to ensure that **the numbers can only be accessed on the machine on which the software was first installed.**" Para. 0151 also unambiguously provides that the numbers **can only be accessed on the machine on which the software was first installed.** This aspect of Flitcroft's patent prevents the unique portability and isolation from intrusion which are important features of the Applicant's patent

The limits described in Flitcroft paras. 56 and 57 are different than those described by the Applicant. Unlike Flitcroft's method, the Applicant's novel method enables impulse purchases - the user can decide on limits in respect of each purchase at the time of making the purchase, i.e. when the user learns the relevant price required by a supplier. In Flitcroft method, the limits are applied in advance by the issuer and the user does not have the opportunity of adjusting these limits according to varying needs of impulse buying while browser shopping on the web.

**Re: claims 20 and 7 (Use of Cybercodes):**



Cybercodes which are also described in claims 7 and 8, are included in the Applicant's provisional applications filed on Feb. 11, 2000, May 22, 2000, Aug 21 2000 and Oct. 10 2000.

**Claim 7** defines the use of Cybercodes in conjunction with a digitally recordable card, whereas **claim 20** refers to a non-digital card such as paper or plastic.

These claims specify that a card number will not be effective unless supplemented by a Cybercode inserted either at the end of said number or in some predetermined position within said number. A list of Cybercodes in a set sequence is allocated to the card number and each time the card number is used it must be associated with the relevant Cybercode in the correct sequence. Flitcroft's paras. 70, 71, 74 and 75, cited by the Examiner, describe a very different method which comprises establishing a list of substitute "limited use" card numbers allocated to a particular customer which are used in place of, not in conjunction with, the customers regular number. This requires a mechanism for associating the master account number with the limited use number when it is received from the user. In the Applicant's invention, the card issuer does not need such mechanism as the regular number is already included in the Cybercoupon that is communicated by the user.

Another important difference is that in Flitcroft's method, substitute numbers are complete and may be used by an unauthorized person into whose hands they may fall. In the Applicant's method, the substitute number or Cybercoupon is composed of two parts, the card number and a Cybercode, each of which may be stored separately. An unauthorized person is unable to use the card number without knowing the specific relevant Cybercode in its correct sequence and vice versa.

An additional advantage of the Applicant's method is that there is no need for encryption as is used by Flitcroft et al.

**Re: claims 10 -13 (encrypted authentication):**

Flitcroft's paras. 134 to 146 contain a general theoretical discussion of common encryption methods, which can be used for encrypting the proxy numbers in a credit card transaction. These methods are known to anyone moderately skilled in the art. The Applicant did not elaborate on the details of the encryption method used as the art of public/private key encryption is widely known and readily available in the literature. The Applicant uses encryption as a publicly available tool, the novelty lying in the unique method of combining encryption with generation of a random number without storing any encryption keys on the user's computer.

The Applicant's claims 10 to 13 inclusive do not relate only to credit card transactions, but to establishing positive authentication of the card holder in two party transactions such as in obtaining card access to a database or to premises or to a vending machine.

When these claims are read in conjunction with Applicant's claims 1, 2 and 3 (2 and 3 now being incorporated in revised claim 1) it is obvious that the novelty does not lie just in using the well known method of public key encryption or digital signatures, but rather in the fact that the encryption keys are protected from hacking as they are not stored on the user's computer but on the removable card. So too can the challenge be generated while the computer is offline and protected from hacking. As is obvious from revised claim 1, the card is disconnected from the computer before it goes online to communicate the challenge to the remote site.

**Re: claim 14 (combined magstripe and smartcard):**

No reference has been found in Flitcroft et al's patent or in Franklin's patent anticipating this claim.

**Re: claims 15 - 18 (DTMF):**

In para. 127 Flitcroft makes a very broad and unspecific reference to communicating by telephone. He states "In the case a device intended for use over the telephone, the number can either be spoken by the user or appropriate tones can be generated to automatically transmit the number to the merchant". It does not suggest or even hint at incorporating a DTMF generator on a physical card, which is not part of the user's computer. Flitcroft's vague general statement and extremely cursory mention of "tones" does not constitute an anticipation of the Applicant's claim.

Flitcroft paras. 283 to 302 contain a general description of known means of conducting purchases by Mail Order or Telephone Orders (MOTO) but these too, do not relate to the specific provision for converting proxy numbers to audio signals by means of a DTMF generator as described in said claims 15 to 18.

**Re: claim 19 (POS):**

It is not clear where Flitcroft relates to the Applicant's claim 19.

**Re: claim 20:**

See claim 7 above.

**Re: claim 21:**

It is not clear where Flitcroft relates to this claim.

**2) 35 U.S.C. 103(a)**

**Re: Claims 2-4 and 9, rejected under 35 U.S.C. 103(a) as being unpatentable over Flitcroft.**

**Re: claims 2 and 3 (Disconnecting the card from the computer and advertising):**

Flitcroft's paras. 117-130 deal generally with the electronic transmission embodiment. Reference to swipe card readers in para. 69 is very cursory. It shows only that credit card transactions can originate from a merchant in the conventional manner, e.g., by swiping a credit card through a card swipe unit. The described manner of using a swipe card does not disconnect the data and program modules on the user's computer from the internet or other online connection and does not bear any similarity to isolation of such programs and data from the internet or other online connection as provided in the Applicant's invention. It is not at all obvious that the reference to swipe cards was intended to minimize any possible online intrusion. Rather it is obvious that the use as described is merely as an input device. It cannot prevent a hacker from stealing the password and other information which Flitcroft describes as being stored on the user's computer and there is no hint that this was the intention.

Re: Advertising on the logon screen (Applicant's original claims 2 and 3, now claim 2). Flitcroft's method as stated in parags. 239 and 241, does not resemble Applicant's method of providing for generation by an executable program on the user's card of advertising which appears in the user's logon screen and Applicant's method is not at all obvious from Flitcroft's method. Flitcroft does not provide for advertising on the user's screen. Rather it provides advertising on the back of a remote access device, RAD 1504 as illustrated in Fig. 15 and as described in Flitcroft 239.

Neither does Franklin's reference to advertising resemble the Applicant's method. This patent merely states "During normal operation on the Web, the customer comes across a banner advertising an online commerce card sponsored by the issuing bank. The banner may be part of the bank's Web site, or part of

a statement to its customers, or included as advertisement in other Web content."

The reference to para. 127 is not understood in relation to inserting the proxy number in the appropriate position on the vendor's form order form.

The procedure described in Applicant's claim 3, (which has now been incorporated into revised claim 1) provides the very highest security level, completely avoiding any connection between the card which generates the proxy numbers and the internet or other online connection. The proxy number is generated and displayed and noted or otherwise recorded while the user's computer is offline. The card is then disconnected or removed from the computer before the computer goes online to communicate the encrypted proxy number. This procedure does not in any way resemble the use of a swipe card for transactions originating from a merchant as described in Flitcroft 102 and 58 which procedure cannot prevent hacking of sensitive data such as passwords and encryption keys that are stored on the user's computer.

**Re: claim 4 (irregular entry of password):**

Merely disabling the program as provided by Flitcroft 148 is a procedure commonly used in many computerized applications. It is very different than the Applicant's procedure of sending an encrypted message notifying the issuer that an irregular attempt has been made to use the card, thus allowing the issuer a choice of appropriate action, which may include communicating with the true owner of the card to establish whether an unintentional error was made. If the use was illegitimate, the perpetrator is left with the impression that a genuine proxy number has been generated, which can be used for a purchase or

other transaction, thus facilitating apprehension of the perpetrator. There is no hint in Flitcroft's application that the Applicant's alert procedure was contemplated and it is not an obvious development of the procedure described by Flitcroft.

**Re: claim 9:**

The Examiner concedes that Flitcroft does not recite the procedure described in Applicant's claim 9 and that such an added method would be of value. The manner in which numbers are allocated as described in Flitcroft 80-98 is completely different from the sequential arrangement described by the Applicant. Flitcroft's card numbers do not bear a similarity to the Applicant's Cybercodes and the methods taught by Flitcroft in said paragraphs to allocate limited use credit/debit card numbers and to provide for numbers being received out of sequence bears no relation to the Applicant's sequential process. Therefore it would not have been obvious to one ordinarily skilled in the art to have added this method as described in claim 9 in order to ensure that Cybercodes maybe authorized out of sequence when they statistically fall within industry accepted standards for the lag times between user report of their use and merchant request for their authorization.

See also claim 7 above.

**Re: claims 5 and 6, rejected under 35 U.S.C. 103(a) as being unpatentable over Flitcroft et al as applied to claim 1 above, and further in view of Franklin et al., US Patent No 6,000,832.**

Flitcroft deals principally with credit card numbers not cards and his application is limited to credit card applications. He does not include general access cards as in the Applicant's invention which is designed as a general means

for authentication in establishing online communication and in which credit cards comprise only a subset of the applications. Flitcroft describes generation of proxy numbers by the issuer, allocating them to the user, then encrypting them at the issuer site, for communication electronically to the user for storage by the user with attendant security risks. This procedure is substantially different than generating the proxy numbers offline by the user, as provided by the Applicant. The Applicant's method of generating the numbers by the user is also completely different from the method described by Flitcroft, e.g. it does not use a database at the issuer, containing a list of proxy numbers issued for matching with the proxy numbers received and with the user's master number.

In Franklin's patent the abstract states "The "card" does not exist in physical form, but instead exists in digital form", whereas the Applicant's invention is essentially based on a physical card.

Flitcroft para. 120, describes the method as allowing secure storage, (not processing), of issued limited use credit/debit/charge card numbers until required by the user. It does not suggest a card containing any computing circuitry. Storage is required of sensitive programs and or data on the user's computer. He states clearly that these numbers can be stored in a variety of encrypted forms, (having been received already encrypted), but he does not claim a card containing an executable program which can perform the encryption as provided in the Applicant's invention. Rather, Flitcroft's method stores numbers, which have been received already encrypted by the issuer as confirmed in para. 0072 which states these limited use numbers can be electronically downloaded to a user's personal computer 104, where they are stored in local memory 142 of the personal computer 104 for subsequent use.

In view of the above considerations it would certainly not have been obvious to one of ordinary skill in the art at the

time the application was made to combine Flitcroft's system with Franklin's so that the Cybercoupons can be generated in the cards themselves.

In the prior art patents cited by the Examiner, elements are stored on the user's computer and are therefore subject to hacking and preclude portability. The methods of these prior art inventions are limited to use only in conjunction with a designated computer.

Thus it should be clear from the above remarks, that the Applicant's invention is not anticipated by the prior art, nor is it an obvious development of the cited prior art.

As stated in the decision in *Re Marshall*, 198 USPQ 344 (1978), "To constitute an anticipation, all material elements recited in a claim must be found in one unit of prior art...". Since the Flitcroft and Franklin references neither 1) identically describe the invention, nor 2) enable one skilled in the art to practice it, Applicant deems the 102(a) rejection improper, and respectfully requests that it be withdrawn.

It is the Applicant's position that the combination of the cited references to form the basis of the Sec. 103(a) rejection is improper, and Applicant respectfully requests that it be withdrawn. In citing the references under Sec. 103(a), the question is raised whether the references would suggest the invention, as stated in the decision of *In Re Lintner* (172 USPQ 560, 562, CCPA 1972);

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the references before him to make the proposed substitution, combination or other modification."

Similarly, *In Re Regel* (188 USPQ 136, CCPA 1975) decided that the question raised under Sec. 103 is whether the prior art taken as a whole would suggest the claimed invention to one of



ordinary skill in the art. Accordingly, even if all the elements of a claim are disclosed in various prior art references, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill would have been prompted to combine the teachings of the references to arrive at the claimed invention.

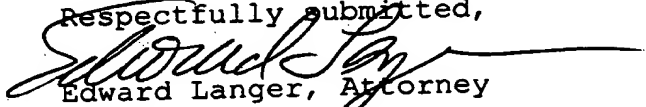
Simply put, and as stated in *In Re Clinton* (188 USPQ 365 CCPA 1976), "do the references themselves... suggest doing what appellants have done", such that there is a requirement that the prior art must have made any proposed modification or changes in the prior art obvious to do, rather than obvious to try.

It is respectfully put forward by the Applicant that there is no reason to consider the prior art references either individually or in combination, as rendering the invention obvious, since none of them discloses a method for secure authentication of a user in a computerized card access transaction via a computer or other device, wherein a physical card issued by a card issuer is embodied in a portable, digitally recordable medium having stored thereon a user program that does not require storage of any passwords, programs, secret keys or any component of said user program on a computer. In this fashion, theft of such passwords or other sensitive information by either an unauthorized person who may gain physical access to the user's computer or by any form of online intrusion is impossible. In addition, the inventive method enables complete portability so that it is not restricted to a specific programmed computer, but is usable in conjunction with any computer equipped with a compatible operating system.

The Applicant has succeeded in overcoming the limitations of computerized card transactions, allowing more secure transactions and furthering the development of e-commerce significantly.

Based on the amendments to the claims and the above remarks, Applicant believes that the invention is novel and inventive and that all the pending claims in the application are deemed to be allowable. Further reconsideration and allowance of the application is respectfully requested at an early date.

Respectfully submitted,

  
Edward Langer, Attorney

Reg. No. 30,564

Shiboleth, Yisraeli, Roberts and Zisman LLP  
350 Fifth Ave., 60<sup>th</sup> Floor  
New York, NY 10118  
212-244-4111  
212-563-7108 fax